Abstract of the Invention

A method of supporting a substantially secure backup copy of a key-server database, said database comprising security information specific to a plurality of users, absent the need for a duplicate key-server is disclosed. According to the method, each individual's security data is stored within the key-server database and is also stored on a portable data storage device, such as a smart card or a PCMCIA token. If the key-server crashes and the database stored thereon is lost, a duplicate key-server database is reconstructed using the aggregate of the partial database files stored on each individual's portable data storage device. Similarly, when a portable data storage device is lost, it can be rebuilt from the data stored within the key-server.